IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
GREENBELT DIVISION

NICHOLAS WALKER
163 Dalma Drive
Mountain View, California 94041

on behalf of himself and all others similarly situated,

Plaintiff,

v.

MARRIOTT INTERNATIONAL, INC. (a Montgomery County, Maryland Resident)
10400 Fernwood Road
Bethesda, Maryland 20817

and

STARWOOD HOTELS AND RESORTS WORLDWIDE, LLC (a Montgomery County, Maryland Resident)
10400 Fernwood Road
Bethesda, Maryland 20817,

Defendants.

CASE NO. 8:18-cv-3702

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Nicholas Walker ("Plaintiff"), on behalf of himself and all others similarly situated, allege the following against Marriott International, Inc. ("Marriott"), Starwood Hotels And Resorts Worldwide, LLC ("Starwood") and any persons or entities acting on their behalf or at their direction or control (collectively "Defendants"). Plaintiff makes these allegations upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE ACTION

1. On November 30, 2018, Marriott International announced that it was subject to one of the largest data breaches in our nation's history when the personal information of up to 500 million hotel guests was exfiltrated from its Starwood guest reservation database as part of an ongoing, four-year long data breach.

2. The information stolen in the breach includes names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, dates of birth, gender, arrival and departure information, reservation dates, and communication preferences. For some, the information also included payment card numbers and payment card expiration dates.

3. During a four-year period, Marriott failed to detect the hackers' presence, notice the massive amounts of data that were being exfiltrated from its databases, or take any steps to investigate the numerous other red flags that should have warned the company about what was happening. As a result of Marriott's failure to protect the consumer information it was entrusted to safeguard, Plaintiff and class members have

been exposed to fraud, identity theft, and financial harm and, as detailed below, are subject to a heightened, imminent risk of such harm in the future.

PARTIES

4. Plaintiff Nicholas Walker is a resident and citizen of Mountain View, California and had his personal information compromised in the data breach after providing it to Defendants to purchase hotel rooms at multiple Starwood hotel properties.

5. Defendant Marriott International, Inc. is organized under the laws of Delaware with its principal place of business in Maryland.

6. Defendant Starwood Hotels and Resorts Worldwide, LLC is organized under the laws of Maryland with its principal place of business in Connecticut.

JURISDICTION AND VENUE

7. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) ("The Class Action Fairness Act") because sufficient diversity of citizenship exists between parties in this action, the aggregate amount in controversy exceeds $5,000,000, and there are 100 or more members of the Class.

8. This Court has personal jurisdiction over Defendants because Marriott maintains its principal place of business in Maryland, Starwood is incorporated in Maryland, and both companies regularly conduct business in Maryland and have sufficient minimum contacts in Maryland.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a) because Marriott's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

The Data Breach

10. Marriott International, Inc. is a leading global lodging company with more than 6,700 properties across 130 countries and territories, reporting revenues of more than $22 billion in fiscal year 2017. Founded in 1927, the company is headquartered outside of Washington, D.C. in Bethesda, Maryland and maintains hotel brands including Marriott, Courtyard and Ritz-Carlton.

11. In September 2016, Marriott completed a $13-billion acquisition of Starwood Hotels & Resorts Worldwide, including its brands of W Hotels, St. Regis, Sheraton Hotels & Resorts, and Westin Hotels & Resorts, among others, to create the world's largest hotel chain. Marriott acknowledged that Starwood's guest loyalty program – Starwood Preferred Guest – was a "central, strategic rationale for the transaction" because the program has loyal members who generally have higher incomes and spend many nights on the road.

12. On November 30, 2018, Marriott confirmed unauthorized access to its Starwood guest reservation database, which contained guest information relating to reservations at Starwood properties on or before September 10, 2018.

13. According to Marriott, it first noticed irregular activity on September 8, 2018 after it received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database.

14. Through investigating the matter, Marriott determined that there had been unauthorized access to the Starwood network since 2014, and that an unauthorized party

had copied and encrypted information, and took steps towards removing it—signaling that the information was carefully exfiltrated by an unauthorized third party.

15. According to cybsercurity blogger Brian Krebs, the hackers likely encrypted the information to avoid detection by any data-loss prevention tools when removing the stolen information from the company's network. Marriott stated that it was later able to decrypt the information and determine that the contents were from the Starwood guest reservation database.

16. Although Marriott says it has not completed its investigation, it acknowledges that the compromised database contains information on up to approximately 500 million guests who made a reservation at a Starwood property.

17. Marriott has further acknowledged that for approximately 327 million of these guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiration dates.

18. Affected individuals include Starwood Preferred Guest members and individuals who provided information to make purchases at a Starwood property, including: W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels. Marriott acknowledged that guests of Starwood branded timeshare properties were also affected.

19. In its privacy policy, Marriott acknowledges that hotel guests must provide their personal information in order to stay at a Marriott/Starwood property and that Marriott seeks "to use reasonable organizational, technical and administrative measures to protect Personal Data."[1] Marriott defines "Personal Data" as "data that identify you as an individual or relate to an identifiable individual."

20. Despite warnings of suspicious network traffic at least as early as September 8, 2018, Marriott did not announce the breach until November 30. By waiting nearly 12 weeks to notify customers, Marriott deprived its customers of an opportunity to take immediate precautions to protect themselves from identity theft and fraud.

Defendants Have a History of Inadequate Data Security Practices

21. Given the amount of sensitive information hotels compile and store, Defendants were well aware they were a target, but nonetheless refused to implement best practices relating to data security—as demonstrated by other data security lapses Defendants have recently experienced.

22. For example, in November 2015, Starwood disclosed that point-of-sale systems at 54 of its hotels located across North America were infected with malware, enabling unauthorized parties to access payment card data of its customers. Starwood issued a press release stating that the "malware affected certain restaurants, gift shops and other point of sale systems at the relevant Starwood properties" but that there was "no indication that our guest reservation or Starwood Preferred Guest membership systems

[1] *See* Marriott Group Global Privacy Statement (last updated May 18, 2018), available at: https://www.marriott.com/about/privacy.mi.

were impacted." The release further stated that: "We take our obligation to safeguard personal information very seriously and are alerting affected customers about this incident so they can take steps to help protect their information."

23. In February 2015, White Lodging Services Corporation, an independent hotel management company used by Marriott, announced that it was investigating a possible data breach after sources in the banking industry began seeing a pattern of fraud on payment cards that were all previously used at Marriott hotels. It was later confirmed that a point-of-sale breach exposed customers' personal information and payment card data at 10 Marriott locations across the country.

24. Following confirmation of the breach, Marriott issued a statement stating that "one of its franchisees has experienced unusual fraud patterns in connection with its systems that process credit card transactions at a number of hotels across a range of brands, including some Marriott-branded hotels." The statement continued: "As this impacts customers of Marriott hotels we want to provide assurance that Marriott has a long-standing commitment to protect the privacy of the personal information that our guests entrust to us, and we will continue to monitor the situation closely."

25. Since that time, there have been numerous additional data breaches targeting the hospitality and accommodation industry, including major hotel chains including Hyatt, Radisson, Hard Rock, and Kimpton, among others. In its recent Data Breach Investigations Report, Verizon noted that 15% of all data breaches occurring in 2017 involved the accommodation and food services industry and that it is "the hardest

hit" industry for point-of sale intrusions. The report noted that there were 338 breaches in the accommodation industry in 2017 alone.

26. On November 2, 2018, Radisson Hotels disclosed a data breach affecting Radisson Rewards members who had their names, company names, e-mail addresses, addresses, phone numbers, Radisson Rewards member numbers and frequent flyer numbers accessed by an unauthorized party.

27. In August 2018, it was announced that China-based Huazhu Hotels Group suffered a massive data breach where the personal information of hundreds of millions of hotel guests was exfiltrated and offered for sale on the dark web.

28. In November 2017, Hilton Worldwide Holdings Inc. agreed to pay $700,000 and bolster security its data security practices for mishandling data breaches in 2014 and 2015, including failing to maintain reasonable data security and failing to notify victims of the data breach in a timely manner. The breaches, discovered in February and July 2015, respectively, exposed the credit card numbers of more than 360,000 guests.

29. In October 2017, Hyatt announced that it discovered unauthorized access to payment card information at 41 of its properties worldwide. This announcement came on the heels of Hyatt's announcement in late 2015 that hackers had gained access to credit card systems at 250 properties in 50 different countries for a period spanning nearly four months, exposing customers' payment card data including cardholder names, numbers, expiration dates, and internal verification codes.

30. In July 2017, multiple hotel chains including Hard Rock Hotels & Casinos, Four Seasons Hotels and Resorts, Trump Hotels, Loews Hotels, Kimpton Hotels &

Restaurants, RLH Corporation and Club Quarter Hotels, among others, reported a data breach via a third-party reservations system provided by Sabre Hospitality Solutions. The breach permitted unauthorized access to customers' credit card information and certain reservation information between August 2016 and March 2017.

31. In February 2017, InterContinental Hotels Group announced that cash registers at more than 1,000 of its properties were infected with malware designed to siphon customers' payment card data from on-site hotel locations between September 29, 2016 and December 29, 2016.

32. In September 2016, Kimpton Hotel & Restaurant Group LLC announced that customers' payment card information was compromised by malware installed on its servers at more than 60 of its hotels and restaurants during a six-month period.

33. In June 2016, Hard Rock Hotel & Casino Las Vegas announced that after receiving reports of fraudulent activity associated with payment cards used at its hotel, the resort conducted an investigation revealing that malware had been installed on its servers allowing unauthorized access to customers' names, credit card numbers, expiration dates, and verification numbers.

34. The following month, Omni Hotels & Resorts confirmed that a similar malware attack exposed the names and payment card information of more than 50,000 customers at 49 of its properties.

35. In addition to data breaches affecting the hospitality industry, Defendants observed numerous other well-publicized data breaches involving major corporations being targeted for consumer information.

36. For example, through a series of data breaches extending back to 2013, more than three billion Yahoo! user accounts were compromised when accountholders' names, addresses, and dates of birth were stolen. The hackers also stole users' passwords, both encrypted and unencrypted, and security questions and answers.

37. In separate incidents in 2013 and 2014, hundreds of millions of retail customers were victimized by hacks of payment card systems at Target and the Home Depot. Both breaches led to rampant payment card fraud and other damages both to consumers and to the card-issuing banks.

38. In summer 2014, a data breach of JP Morgan Chase compromised the data of 76 million American households and 7 million small businesses. Breached data included contact information (names, addresses, phone numbers, and email addresses) as well as internal information about the users.

39. In early 2015, Anthem, the second-largest health insurer in the United States, suffered a data breach that exposed the names, addresses, Social Security numbers, dates of birth, and employment histories of nearly 80 million current and former plan members.

40. And in September 2017, credit reporting agency Equifax announced that hackers stole the personal and financial information of nearly 150 million Americans between May and July 2017.

41. Despite being a holder of customer information for millions of individuals worldwide, Defendants failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to its highly-sensitive

customer information. Defendants had the resources to prevent a breach and made significant expenditures to market their hotels and hospitality services, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches affecting the hospitality industry.

The Effect of the Data Breach on Defendants' Victims

42. The ramifications of Defendants' failure to protect the personal information of its customers are severe. Identity thieves can use the information stolen in the data breach to perpetrate a wide variety of crimes, including tax fraud, identity theft such as opening fraudulent credit cards and loan accounts, as well as various types of government fraud such as changing immigration status using the victim's name, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, obtaining a job, procuring housing, or even giving false information to police during an arrest. In the medical context, consumers' stolen personal information can be used to submit false insurance claims, obtain prescription drugs or medical devices for black-market resale, or get medical treatment in the victim's name. Some of this activity may not come to light for years.

43. The processes of discovering and dealing with the repercussions of identity theft are time-consuming and difficult. The Department of Justice's Bureau of Justice statistics found that "among victims who had personal information used for fraudulent

purposes, 29% spent a month or more resolving problems."[2] Likewise, credit monitoring services are reactive, not preventative, meaning they cannot catch identity theft until after it happens.

44. Additionally, there is commonly lag time between when harm occurs and when it is discovered, and also between when personal information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches, "law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[3]

45. A cyber black market exists in which criminals openly post and sell stolen consumer information on underground Internet websites known as the "dark web"—exposing consumers to identity theft and fraud for years into the future.

46. Defendants' actions and failures to act when required have caused Plaintiff and members of the classes to suffer harm and/or face the significant and imminent risk of future harm, including:

---

[2] Erika Harrell and Lynn Langton, *Victims of Identity Theft, 2012*, (Bureau of Justice Statistics), Dec. 2013, http://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited November 30, 2018).

[3] U.S. Government Accountability Office, GAO Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, at 29, June 2007, http://www.gao.gov/new.items/d07737.pdf (last visited November 30, 2018).

a. Theft of their personal information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. Costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

d. Unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from potential fraud and identify theft posed by their personal information being placed in the hands of criminals;

h. Damages to and diminution in value of their personal information entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff and class members' information against theft and not allow access and misuse of their data by others;

i. Continued risk of exposure to hackers and thieves of their personal information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff and members of the class.

47. Consequently, victims of this breach are at an imminent risk of fraud and identity theft for years to come. Plaintiff and members of the classes defined below have

been harmed and are subject to an increased and concrete risk of further identity theft as a direct result of Defendants' exposure of their personal information.

CLASS ACTION ALLEGATIONS

48. Plaintiff seeks relief in his individual capacity and as a representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and/or (c)(4), Plaintiff brings this action on behalf of himself and the classes preliminarily defined as:

> All U.S. individuals who submitted their personal information to Defendants and whose personal information was compromised as a result of the data breach announced on or about November 30, 2018 (the "Class").
>
> All residents of California who submitted their personal information to Defendants and whose personal information was compromised as a result of the data breach announced on or about November 30, 2018 (the "California Subclass").

49. Excluded from the classes are the Defendants, including any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants. Also excluded are the judges and court personnel in this case and any members of their immediate families.

50. **Numerosity**. Fed. R. Civ. P. 23(a)(1). The members of the classes are so numerous that the joinder of all members is impractical. As reported by Defendants, the breach affects hundreds of millions of Defendants' customers.

51. **Commonality**. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the classes, which predominate over any questions affecting only

individual class members. These common questions of law and fact include, without limitation:

a. Whether Defendants owed a duty to Plaintiff and members of the classes to adequately protect their personal information and to provide timely and accurate notice of the data breach to Plaintiff and members of the classes;

b. Whether Defendants knew or should have known that its systems were vulnerable to attack;

c. Whether Defendants conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of hundreds of millions of customers' personal information;

d. Whether Plaintiff and members of the classes suffered injury, including ascertainable losses, as a result of Defendants' conduct or failure to act;

e. Whether Defendants' information storage and protection protocols were reasonable and compliant with industry standards;

f. Whether Defendants' conduct constituted unfair and deceptive trade practices actionable under the applicable consumer protection laws;

g. Whether Defendants violated statutory obligations by failing to take all reasonable steps to dispose, or arrange for the disposal, of customers' personal information within its custody or control when the records should no longer have been retained by Defendants;

h. Whether Plaintiff and members of the classes are entitled to recover actual damages and/or statutory damages; and

i. Whether Plaintiff and members of the classes are entitled to equitable relief, including injunctive relief, restitution, and disgorgement.

52. All members of the proposed classes are readily ascertainable by objective criteria. Defendants have access to addresses and other contact information for members of the classes, which can be used for providing notice to many class members.

53. **Typicality**. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other class members because Plaintiff's personal information, like that of other class members, was misused and/or disclosed by Defendants.

54. **Adequacy of Representation**. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the members of the classes. Plaintiff's counsel is competent and experienced in litigating class actions, including multiple class actions involving large data breaches.

55. **Superiority of Class Action**. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the classes is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

56. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go likely un-remedied without certification of the classes.

57. Class certification is also appropriate under Fed. R. Civ. P. 23 because Defendants have acted or has refused to act on grounds generally applicable to the classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the classes as a whole.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

58. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

59. Plaintiff brings this cause of action on behalf of the Class.

60. In collecting the personal information of Plaintiff and the Class, Defendants owed those individuals a duty to exercise reasonable care in safeguarding and protecting that information. This duty included, among other things, maintaining and testing Defendants' security systems and taking other reasonable security measures to protect and adequately secure the personal information of Plaintiff and the Class from unauthorized access and use.

61. Defendants' security systems and procedures for handling the personal information of customers were intended to affect Plaintiff and the Class. Defendants were aware that by gathering and storing such sensitive information, they had a responsibility to take reasonable security measures to protect the data from being stolen.

62. Defendants further had a duty to timely disclose to Plaintiff and the Class that their personal information had been or was reasonably believed to have been compromised. Timely disclosure is appropriate so that Plaintiff and the Class could, among other things, monitor their credit reports for identity fraud, obtain credit freezes, undertake appropriate measures to avoid unauthorized charges on their debit card or credit card accounts, and change or cancel their debit or credit card PINs (personal

identification numbers) to prevent or mitigate the risk of fraudulent cash withdrawals or unauthorized transactions.

63. Defendants further had a duty to destroy the personal information of Plaintiff and the Class from its databases within a reasonable amount of time after it was no longer necessary for Defendants to retain such information in order to mitigate the risk of loss of customers' personal information in the event of a data breach.

64. Defendants breached their duty to exercise reasonable care in protecting the personal information of Plaintiff and the Class by failing to implement and maintain adequate security measures to safeguard such information, failing to monitor its systems to identify suspicious activity, allowing unauthorized access to the personal information of Plaintiff and the Class, and failing to adequately encrypt or otherwise prevent unauthorized access to such personal information. Defendants further breached their duty to timely notify Plaintiff and the Class about the data breach.

65. As a direct and proximate result of Defendants' failure to exercise reasonable care and use commercially reasonable security measures, the personal information of Plaintiff and the Class was accessed by unauthorized individuals who are likely to use the information to commit identity theft and fraud. But for Defendants' failure to implement and maintain adequate security measures to protect customers' personal information and failure to monitor its systems to identify suspicious activity, the personal information of Plaintiff and Class would not have been stolen and they would not be at a heightened risk of identity theft and fraud.

66. Plaintiff and the Class have also suffered economic damages, including the purchase of credit monitoring services they would not have otherwise purchased, and spent significant time addressing the effects of identity theft and fraud as well as taking preventative measure like notifying the IRS and credit reporting agencies.

67. Neither Plaintiff nor members of the Class contributed to the data breach, nor did they contribute to Defendants' employment of insufficient security measures to safeguard customers' stored personal information.

68. There is a causal connection between Defendants' failure to implement reasonable security measures to protect customers' personal information and the injury to Plaintiff and the Class. When individuals have their personal information stolen and used to apply for and/or open fraudulent accounts, they are at risk for additional identity theft, and are justified in purchasing credit monitoring services and other services to determine whether identity theft has or will occur.

69. The policy of preventing future harm weighs in favor of finding a special relationship between Defendants and the Class. Plaintiff and members of the Class who provided their personal information to Defendants relied on Defendants to keep their information safe and secured. If companies are not held accountable for failing to take reasonable security measures to protect their customers' personal information, then they will not take the steps that are necessary to protect against future cyber-attacks and data breaches.

70. It was foreseeable that if Defendants did not take reasonable security measures, the personal information of Plaintiff and the Class would be stolen. Hotel

chains like Defendants face a high threat of security breaches due in part to the large amounts and type of information they store and the value of such information on the black market. Defendants should have known to take all reasonable precautions to secure its customers' personal information, especially in light of recent data breaches and publicity regarding cyberattacks.

71. Defendants' negligence was a substantial factor in causing harm to Plaintiff and members of the class.

72. Plaintiff and the Class seek compensatory damages and punitive damages with interest, nominal damages, the costs of suit and attorneys' fees, and other and further relief as this Court deems just and proper.

SECOND CAUSE OF ACTION
Negligence Per Se
(On Behalf of Plaintiff and the Class)

73. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

74. Plaintiff brings this cause of action on behalf of the Class.

75. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as Defendants of failing to use reasonable measures to protect personal information. Various FTC publications and orders also form the basis of Defendants' duty.

76. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect personal information and not complying

with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of personal information it obtained and stored and the foreseeable consequences of a data breach at the world's largest hotel chain.

77. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

78. Plaintiff and the Class are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

79. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

80. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Breach of Contract
(On Behalf of Plaintiff and the Class)

81. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

82. Plaintiff brings this cause of action on behalf of the Class.

83. Marriott's privacy statement represents that it "seeks to use reasonable organizational, technical and administrative measures to protect Personal Data."

84. Marriott's privacy policies constitute an agreement between Defendants and members of the Class.

85. Defendants breached their agreement with Plaintiff and the Class to protect their personal information by (1) failing to implement security measures designed to prevent this attack, (2) failing to employ security protocols to detect the unauthorized network activity, and (3) failing to maintain basic security measures such as complex data encryption so that if data were accessed or stolen it would be unreadable.

86. Plaintiff and the Class have been damaged by Defendants' breach of their contractual obligations because their personal information has been compromised and they have suffered identity theft and fraud, and/or are at an increased risk for identity theft and fraud. Plaintiff and the Class have been deprived of the value of their personal information and have lost money and property as a result of Defendants' unlawful and unfair conduct.

87. Plaintiff individually and on behalf of the Class seeks recovery for damages suffered by members of the class, equitable relief, and injunctive relief requiring Defendants to implement safeguards consistent with its contractual promises.

FOURTH CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

88. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

89. Plaintiff brings this cause of action on behalf of the Class and to the extent necessary, in the alternative to their breach of contract claim.

90. When Plaintiff and Class members paid money and provided their personal information to Defendants in exchange for services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

91. Defendants solicited and invited prospective hotel guests and other consumers to provide their personal information as part of its regular business practices. These individuals accepted Defendants' offers and provided their personal information to Defendants. In entering into such implied contracts, Plaintiff and the Class assumed that Defendants' data security practices and policies were reasonable and consistent with industry standards, and that Defendants would use part of the funds received from Plaintiff and the Class to pay for adequate and reasonable data security practices.

92. Plaintiff and the Class would not have provided and entrusted their personal information to Defendants in the absence of the implied contract between them and Defendants to keep the information secure.

93. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendants.

94. Defendants breached their implied contracts with Plaintiff and the Class by failing to safeguard and protect their personal information and by failing to provide timely and accurate notice that their personal information was compromised as a result of a data breach.

95. As a direct and proximate result of Defendants' breaches of their implied contracts, Plaintiff and the Class sustained actual losses and damages as described herein.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

96. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

97. Plaintiff brings this cause of action on behalf of the Class and to the extent necessary, in the alternative to their breach of contract claims.

98. Plaintiff and the Class conferred a monetary benefit on Defendants in the form of money paid to Defendants for their services. Plaintiff and the Class also provided their personal information to Defendants which Defendants utilized for monetary purposes.

99. Defendants appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class.

100. The money paid by Plaintiff and the Class paid to Defendants should have been used by Defendants, in part, to pay for the costs of reasonable data privacy and security practices and procedures.

101. As a result of Defendants' conduct, Plaintiff and the Class suffered actual damages in an amount equal to the difference in value between services with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and the inadequate services without reasonable data privacy and security practices and procedures that they received.

102. Under principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and class members because Defendants failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and the Class paid for.

103. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds received by it.

104. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendants traceable to Plaintiff and the Class.

SIXTH CAUSE OF ACTION
Violation of the Maryland Personal Information Protection Act and Consumer Protection Act, Maryland Code Commercial Law §§ 13-101 *et seq*., 14-3501 *et seq*.
(On Behalf of Plaintiff and the Class)

105. Plaintiff incorporates the above allegations by reference.

106. Plaintiff brings this cause of action on behalf of the Class.

107. Defendants are incorporated and/or headquartered in Maryland and are subject to the laws of Maryland. Pursuant to the Maryland Personal Information Protection Act (PIPA), Maryland businesses have a statutory obligation to maintain the security of personal information of individuals.

108. "[T]o protect personal information from unauthorized access, use, modification, or disclosure," the Maryland Legislature enacted PIPA, Maryland Code, Commercial Law § 14-3503(a), which requires that any business that "owns or licenses personal information of an individual residing in the State shall implement and maintain

reasonable security procedures and practices appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations."

109. As described herein, Defendants failed to implement and maintain reasonable security procedures and practices to protect the personal information of Plaintiff and the Class, and thereby violated Maryland Code, Commercial Law § 14-3503(a).

110. The PIPA further provides that in the event of a security breach, notice must be given to consumers as soon as reasonably practicable following the investigation. The notice sent to consumer must include: a description of the information compromised; contact information for the business, including a toll-free number if the business has one; toll-free numbers and addresses for each of the three credit reporting agencies: Equifax, Experian and TransUnion; toll-free numbers, addresses and websites for the FTC and the Office of the Attorney General. *See* Maryland Code, Commercial Law § 14-3504.

111. Prior to sending notification to consumers, PIPA states that a business must notify the Office of the Attorney General that includes a brief description of the nature of the security breach, the number of Maryland residents being notified, what information has been compromised, and any steps the business is taking to restore the integrity of the system. *See id*.

112. As described above, Defendants did not timely notify affected individuals that they were subject to a data breach.

113. Under Maryland Code, Commercial Law section 14-3508, Defendants' violations of the PIPA also constitute unfair or deceptive trade practices prohibited by the

Maryland Consumer Protection Act, and subject to the Consumer Protection Act's enforcement provisions.

114. Accordingly, Defendants are liable to Plaintiff and the Class for damages and attorneys' fees under Maryland Code, Commercial Law § 13-408.

115. Plaintiff and the Class seek all remedies available under Maryland law, including but not limited to, damages and attorneys' fees.

SEVENTH CAUSE OF ACTION
Violation of the California Customer Records Act,
California Civil Code Section 1798.80, *et seq.*
(On Behalf of the California Subclass)

116. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

117. Plaintiff brings this cause of action on behalf of the California Subclass.

118. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted Civil Code § 1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

119. Defendants are "businesses" within the meaning of Civil Code § 1798.80(a).

120. Plaintiff and members of the California Subclass are "individual[s]" within the meaning of the Civil Code § 1798.80(d). Pursuant to Civil Code §§ 1798.80(e) and

1798.81.5(d)(1)(C), "personal information" includes an individual's name, Social Security number, driver's license or state identification card number, debit card and credit card information, medical information, or health insurance information. "Personal information" under Civil Code § 1798.80(e) also includes address, telephone number, passport number, education, employment, employment history, or health insurance information.

121. The breach of the personal information of hundreds of millions customers constituted a "breach of the security system" of Defendants pursuant to Civil Code § 1798.82(g).

122. By failing to implement reasonable measures to protect the personal information of Plaintiff and the California Subclass, Defendants violated Civil Code § 1798.81.5.

123. In addition, by failing to take all reasonable steps to dispose, or arrange for the disposal, of customers' information within its custody or control when that information no longer should have been retained by Defendants, Defendants violated Civil Code § 1798.81.

124. In addition, by failing to promptly notify all affected individuals that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the data breach, Defendants violated Civil Code § 1798.82 of the same title. Defendants' failure to timely notify affected individuals of the breach has caused damage to class members who have had to buy identity protection services or take other measures to remediate the effects of the breach.

125. By violating Civil Code §§ 1798.81.5, 1789.81 and 1798.82, Defendants "may be enjoined" under Civil Code § 1798.84(e).

126. Accordingly, Plaintiff requests that the Court enter an injunction requiring Defendants to implement and maintain reasonable security procedures to protect customers' personal information in compliance with the California Customer Records Act, including, but not limited to: (1) ordering that Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis; (2) ordering that Defendants engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning and security checks; (5) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (6) ordering Defendants to meaningfully educate affected individuals about the threats they face as a result of the loss of their personal information to third parties, as well as the steps they must take to protect themselves; and (7) ordering Defendants to adequately encrypt sensitive personal information.

127. Plaintiff further requests that the Court require Defendants to (1) identify and notify all members of the California Subclass regarding the existence and effects of

the data breach; and (2) to notify affected individuals of any future data breaches by email within 24 hours of Defendants' discovery of a breach or possible breach and by mail within 72 hours.

128. As a result of Defendants' violation of Civil Code §§ 1798.81.5, 1798.81 and 1798.82, Plaintiff and the California Subclass have and will incur economic damages relating to time and money spent remedying the breach, including but not limited to, expenses for bank fees associated with the breach, any unauthorized charges made on financial accounts, lack of access to funds while banks issue new cards, tax fraud, as well as the costs of credit monitoring and purchasing credit reports.

129. Plaintiff, individually and on behalf of the members of the California Subclass, seeks all remedies available under Civil Code § 1798.84, including, but not limited to damages suffered by members of the class, equitable relief, and reasonable attorneys' fees and costs under applicable law.

EIGHTH CAUSE OF ACTION
Unlawful and Unfair Business Practices Under California Business and Professions Code § 17200, *et seq.*
(On Behalf of the California Subclass)

130. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

131. Plaintiff brings this cause of action on behalf of the California Subclass.

132. Defendants' acts and practices, as alleged in this Complaint, constitute unlawful and unfair business practices, in violation of the Unfair Competition Law

("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq.*, and because Defendants' conduct was negligent:

a. Defendants' practices were unlawful and in violation of California Civil Code § 1798.81.5(b) because Defendants failed to take reasonable security measures in protecting customers' personal information;

b. Defendants' practices were unlawful and in violation of California Civil Code § 1798.81 because Defendants failed to take all reasonable steps to dispose, or arrange for the disposal, of customers' records within its custody or control containing personal information when the records should no longer have been retained by Defendants;

c. Defendants' practices were unlawful and in violation of California Civil Code § 1798.82 because Defendants have unreasonably delayed informing Plaintiff and the California Subclass about the breach of security after Defendants knew the data breach occurred; and

d. Defendants' practices were unlawful and in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) because Defendants adopted unreasonable data security practices that constitute unfair and deceptive acts and practices in and affecting commerce.

133. The acts, omissions, and conduct of Defendants constitute a violation of the unlawful prong of the UCL because Defendants failed to comport with a reasonable standard of care and California public policy as reflected in statutes such as the Information Practices Act of 1977, Cal. Civ. Code § 1798, *et seq.*, and California Customer Records Act, which seek to protect customers' data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

134. In failing to protect customers' personal information and unduly delaying informing them of the data breach, Defendants have engaged in unfair business practices by engaging in conduct that undermines or violates the stated policies underlying the California Customer Records Act and the Information Practices Act of 1977. In enacting

the California Customer Records Act, the Legislature stated that: "[i]dentity theft is costly to the marketplace and to consumers" and that "victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative." 2002 Cal. Legis. Serv. Ch. 1054 (A.B. 700). Defendants' conduct also undermines California public policy as reflected in other statutes such as the Information Practices Act of 1977, Cal. Civ. Code § 1798, *et seq*., which seeks to protect customers' data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

135. As a direct and proximate result of Defendants' unlawful and unfair business practices as alleged herein, Plaintiff and the California Subclass have suffered injury in fact. Plaintiff and the California Subclass have been injured in that their personal information has been compromised and used to conduct identity theft and fraud, and they are at an increased risk for additional future identity theft and fraud. Plaintiff and the California Subclass have also lost money and property mitigating the effects of the breach by purchasing credit monitoring and other services they would not otherwise had to but for Defendants' unlawful and unfair conduct.

136. As a direct and proximate result of Defendants' unlawful and unfair business practices as alleged herein, Plaintiff and the California Subclass face continued identity and theft and an increased risk of future identity theft based on the theft and disclosure of their personal information.

137. Because of Defendants' unfair and unlawful business practices, Plaintiff and the California Subclass are entitled to relief, including restitution for costs incurred

associated with the data breach and disgorgement of all profits accruing to Defendants because of its unlawful and unfair business practices, declaratory relief, and a permanent injunction enjoining Defendants from its unlawful and unfair practices.

138. The injunctive relief that Plaintiff and the California Subclass are entitled to includes, but is not limited to: (1) ordering that Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis; (2) ordering Defendants engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning and security checks; (5) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (6) ordering Defendants to meaningfully educate affected individuals about the threats they face as a result of the loss of their personal information to third parties, as well as the steps they must take to protect themselves; and (7) ordering Defendants to adequately encrypt sensitive personal information.

139. Plaintiff, individually and on behalf of the members of the California Subclass, also seeks reasonable attorneys' fees and costs under applicable law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the classes set forth herein, respectfully requests the following relief:

a. That the Court certify this case as a class action pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and/or (c)(4), pursuant to Fed. R. Civ. P. 23(g), appoint the named Plaintiff to be the Class representative and the undersigned counsel to be Class counsel;

b. That the Court award Plaintiff and the classes appropriate relief, including actual and statutory damages, restitution and disgorgement;

c. That the Court award Plaintiff and the classes equitable, injunctive and declaratory relief as may be appropriate under applicable state laws;

d. That the Court award Plaintiff and the classes actual damages, compensatory damages, nominal damages, statutory damages, and statutory penalties, to the full extent permitted by law, in an amount to be determined;

e. That the Court award Plaintiff and the classes pre-judgment and post-judgment interest;

f. That the Court award Plaintiff and the classes reasonable attorneys' fees and costs as allowable by law; and

g. That the Court award Plaintiff and the classes such other, favorable relief as allowable under law or at equity.

JURY DEMAND

Plaintiff hereby demands a jury trial in the instant action.

Dated: November 30, 2018

Respectfully submitted,

By: _____

Hassan Zavareei (No. 18489)
TYCKO & ZAVAREEI LLP
1828 L. Street, NW, Suite 1000
Washington, DC 20036
hzavareei@tzlegal.com
Tel: (202) 973-0910
Fax: (202) 973-0950

/s/ Norman E. Siegel
Norman E. Siegel
Barrett J. Vahle
J. Austin Moore
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City MO 64112
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com
Tel: (816) 714-7100
Fax: (816) 714-7101

Counsel for Plaintiff and the Class